Network Working Group
Internet-Draft
Intended status: Informational
Expires: 26 October 2026

S. Nurpmeso, Ed.
24 April 2026

Delivered-Enc Email Header Field
draft-nurpmeso-delivered-enc-00

Abstract

Cryptographically protected email aims in hiding and protecting. Extending this to an uppermost extend also for trace headers, and/or the transport layer, so that only directly involved hops, which need to have a notion to "know", the sending system and/or the receiving system thus, can interpret certain header information, is important. This document ensures that only the receiving system, in its desire to prevent email loops, can interpret the real content of the delivery notice header.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 26 October 2026.

Copyright Notice

Table of Contents

1. Introduction

The SMTP[RFC5321] protocol documents in section 6.3 "Loop Detection" an approach to prevent infinite email loops. In operational practice explicit trace header fields were in use for decades, to record delivery addresses, and to shortcut loop detection, and avoid simple counting mechanisms, until [RFC9228] created an IETF document by describing one of the solutions used in practice, the Delivered-To Email Header Field.

2. Encrypting information to protect email

This document introduces a new header field that has the same purpose, and (likely) records the same information that RFC 9228 describes, it however encourages systems to encrypt any content the header field might have, and produce and store solely BASE64[RFC4648] encoded output. Only the local system (any party owning the encryption key) will be capable to decrypt the real content in this scenario, and therefore only interested parties for which the information makes sense.

3. Delivered-Enc

The syntax of the header field is:

"Delivered-Enc:" FWS BASE64 FWS CRLF ; BASE64 from RFC4648

4. IANA Considerations

This document would request the header field name "Delivered-Enc" from IANA.

5. References

5.1. Normative References

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[RFC5321] Klensin, J., "Simple Mail Transfer Protocol", RFC 5321, DOI 10.17487/RFC5321, October 2008, <https://www.rfc-editor.org/info/rfc5321>.

[RFC9228] Crocker, D., Ed., "Delivered-To Email Header Field", RFC 9228, DOI 10.17487/RFC9228, April 2022, <https://www.rfc-editor.org/info/rfc9228>.

Author’s Address

Steffen Nurpmeso (editor)
Email: steffen@sdaoden.eu